NEW YORK TIMES
26 February 1986

U.S. Computer Security Viewed as Inadequate

By DAVID BURNHAM
Special to The New York Times

WASHINGTON, Feb. 25 — Night after night, Tyson Jolliffe, the Federal official in charge of computer security at the Immigration and Naturalization Service, sat at the kitchen table in his home in Leesburg, Va., tapping at his small computer.

Mr. Jolliffe was not just another computer enthusiast. Instead, Government investigators now know that he was using his agency's computer in Washington to generate fraudulent immigration documents, which he then sold to illegal immigrants. They estimate that he and his confederates earned at least $800,000 before they were caught and sent to prison.

The Jolliffe case illustrates the central conclusion of two new Government studies: the Federal Government's computers are open to manipulation and fraud and the experts working for Federal agencies may be the most serious threat.

In a study to be made public Wednesday at a hearing of the Senate Governmental Affairs Committee, the Office of Technology Assessment concludes there was widespread evidence that the effort for "appropriate information systems security measures" has been ineffective.

'New Levels of Risk'

The technology office, a research arm of Congress, says the failure of Government planners and the rapid growth of computerized information means Federal agencies now faced "fundamentally new levels of risk."

The study adds that although a great deal of attention has been focused on outside computer experts, security officials "are nearly unanimous in their view that the more significant security problem is abuse of information systems by those authorized to use them."

A similar judgment was voiced in the first annual report of the the National Telecommunications and Information Security Committee, a special Government-wide organization created two years ago. In a public version of the report, the committee said the protection given to both secret and sensitive information was "unsatisfactory" and that the overall security situation was "poor and rapidly getting worse."

The committee's report said the majority of crimes against Government computers were committed by Government employees.

Number of Computers Rises

The situation is viewed as particularly serious because of rapid growth. In the last few years, for example, the number of big computers has more than doubled, from 11,000 in 1980 to 27,000 in 1985. In the same period, the number terminals booked into these computers has more than quadrupled and the number of small computers has grown from a few thousand to at least 100,000.

Walter P. Connery, the director of the Office of Professional Responsibility in the immigration service, described how Mr. Jolliffe and several allies had produced and sold fraudulent permament alien resident documents to illegal immigrants.

"There is a failure in our system that is very common throughout Government: it has no audit trail," said Mr. Connery, a former deputy inspector of the New York Police Department.

He said that while changes had been made after the accidental discovery of Mr. Jolliffe's scheme "the jury is out whether the system actually is any more secure."

According to the investigator, the essential element in the fraud was the ability to find alien resident numbers that had not been assigned to someone. Mr. Connery said that Mr. Jolliffe, using his home computer, wrote a program that ordered the Government computer to search the files for unused numbers. These were sent to the agency's production facility in Texas.

Mr. Connery said that in the last three years his office investigated more than 100 document fraud cases that resulted in the conviction of 17 people, four of whom used the agency's computer as part of their schemes.

After a trial last summer in Federal Court in the District of Columbia, Mr. Jolliffe was sentenced to five years in prison.

According to a survey by the Office of Technology Assessment, 13 major Federal departments and 20 independent agencies last year spent $33.5 million for security projects for computers and communication devices, four times what they spent in 1980.

The overall conclusion of the office was particularly pessimistic.

Many Do Not Screen Personnel

A survey conducted by the office found that a quarter of the agencies handling sensitive but not secret information did not screen the background of people with access to the computer systems, about half did not have restrictions on the ability to get into the system by dialing a number and that three-quarters of the agencies had no security policy for small computers.

Senator Bill Cohen, Republican of Maine, chairman of Governmental Affairs Oversight Subcommittee, said he was concerned by the finding that 40 percent of the agencies had not conducted vulnerability tests and that 60 percent did not have contingency plans in the event their systems were disabled.

The annual report of the Federal Government's National Telecommunications and Information Committee was completed last September. But a public version of the report has been circulating among Federal agencies only in the last few weeks.